IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Paul Gassoway
Serial No.:	10/849,318
Filing Date:	May 19, 2004
Group Art Unit:	2436
Confirmation No.:	5789
Examiner:	Oscar A. Louie
Title:	***Method and System for Computer Security***

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Appellant has appealed to the Board of Patent Appeals and Interferences ("*Board*") from the Final Office Action dated May 26, 2010 ("*Final Office Action*") and the Advisory Action dated August 9, 2010 finally rejecting Claims 1-24. Appellants filed a Notice of Appeal in this matter on August 26, 2010.

REAL PARTY IN INTEREST

This Application is currently owned by Computer Associates Think, Inc. as indicated by:

an assignment recorded on 02/10/2005 from inventor Paul Gassoway to Computer Associates Think, Inc., in the Assignment Records of the PTO at Reel 016311, Frame 0256 (3 pages).

RELATED APPEALS AND INTERFERENCES

To the knowledge of Appellant's counsel, there are no known interferences or judicial proceedings that will directly affect or be directly affected by or have a bearing on the Board's decision regarding this Appeal.

STATUS OF CLAIMS

Claims 1-24 are pending and stand rejected pursuant to a Final Office Action dated May 26, 2010 ("*Final Office Action*").

Specifically, the Examiner rejects Claims 1-4, 7-10, 13-16, and 19-22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,279,113 to Vaidya ("*Vaidya*") in view of U.S. Patent Publication No. 2005/0037733 to Coleman et al ("*Coleman*").

For the reasons discussed below, Appellant respectfully submits that the rejections of Claims 1-24 are improper and should be reversed by the Board. Accordingly, Appellant presents Claims 1-24 for Appeal. All pending claims are shown in Appendix A, attached hereto.

STATUS OF AMENDMENTS

All amendments submitted by Appellant have been entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

Figure 1 shows an example of a computer system 100 which may implement the method and system of the present disclosure. The system and method of the present disclosure may be implemented in the form of a software application running on a computer system, for example, a mainframe, personal computer (PC), handheld computer, server, etc. The software application may be stored on a recording media locally accessible by the computer system, for example, floppy disk, compact disk, hard disk, etc., or may be remote from the computer system and accessible via a hard wired or wireless connection to a network, for example, a local area network, or the Internet. (*Specification*, Page 7, lines 6-13).

The computer system 100 can include a central processing unit (CPU) 102, program and data storage devices 104, a printer interface 106, a display unit 108, a (LAN) local area network data transmission controller 110, a LAN interface 112, a network controller 114, an internal bus 116, and one or more input devices 118 (for example, a keyboard, mouse etc.). As shown, the system 100 may be connected to a database 120, via a link 122. (*Specification*, Page 7, lines 14-18).

Attacks against a computer system often involve a large number of penetration attempts and/or probing before the attack succeeds in infiltrating the system. According to an embodiment of the present disclosure, as the present system receives more suspicious traffic, it is more likely to block the suspicious activity while still allowing normal traffic to pass through. (*Specification*, Page 7, lines 19-23).

Figure 2 is a block diagram for describing various aspects of embodiments of the present disclosure. A system for maintaining computer security 303 resides between two networks. For example, according to this embodiment, system 303 resides between the Internet 301 and an internal network 302. Of course, system 303 may also reside between two or more internal networks and/or the internet. System 303 passes data back and forth between the Internet 301 and the internal network 302. In this way, system 303 can selectively prevent data from entering and/or leaving the internal network 302. (*Specification*, Page 8, lines 1-7).

According to an embodiment of the present disclosure, system 303 includes an intrusion protection system combining a firewall 305 and an intrusion detection system (IDS)

307. IDS 307 uses signatures to determine whether packets may be malicious. Each of the IDS signatures has a certainty level associated with it. System 303 also has a certainty level associated with it. If a packet is found that matches a signature and the certainty level of the matched signature exceeds the certainty level of system 303, system 303 blocks or discards the packet. Attacks often begin with suspicious activity as the attacker probes the network for vulnerabilities. As system 303 receives more suspicious activity, it reduces its certainty level, so that it is more likely to block the actual attack when it occurs. (*Specification*, Page 8, lines 8-16).

The certainty level of the signatures may be determined using a number of factors, including precision of the signature, length of the signature, and/or developer assigned value, etc. For example, a relatively lengthy precise signature will have a higher level of certainty than a shorter imprecise signature. In the alternative, each signature may be assigned the same certainty level. The certainty level of the system 303 (system certainty level) acts as a variable threshold and is based upon the amount of matching traffic that the system has encountered before. For example, the more packets having a matching signature that system 303 encounters, the lower the system certainty level is. When a packet matches a signature, and the signature's certainty level exceeds the system's certainty level, the system blocks the packet. (*Specification*, Page 8, line 17 through Page 9, line 3).

Figure 3 is a block diagram and Figure 4 is a flow chart illustrating a system and method for maintaining computer security, according to an embodiment of the present disclosure. System 303 includes a database 402 of signatures of known malicious data. As described above, each signature in the signature database 402 is assigned a signature certainty level. Database 402 my be included in system 303 or may be remote from and accessible by system 303. The data 401 is received and compared with the signatures (Step S40) located in signature database 402 by signature comparison module 404. According to an embodiment of the present disclosure, the data 401 may be packets of data. If the data 401 does not match a signature found in the signature database 402 (No, Step S42), then the certainty level of the system 303 is increased (Step S44) by incrementing/decrementing system certainty level module 405 and the data 401 is forwarded on. (*Specification*, Page 9, lines 4-14).

If a match is found in the signature database 402 (Yes, Step S42), then the certainty level of the system 303 is decreased (Step S43) by module 405. The signature certainty level of the matching signature is then compared to the system certainty level (Step S48) by signal

certainty and system certainty level comparison module 406. If the signature certainty level is greater than the system certainty level (Yes, Step S50), then the data 401 is discarded. For example, the data may be discarded to a bit bucket 403. However, if after decreasing the system certainty level, the signature certainty level is not greater than the signature certainty (No, Step S50), then the data 401 is forwarded on. A log may be kept to keep a record of data that was forwarded that matched a signature. Information may also be sent to the destination of the packet indicating that the packet matched a signature and may possibly be malicious. Each time the system tests subsequent data, the increased or decreased system certainty level set by the previous data becomes the new system certainty level. Thus, the more suspicious activity the system receives, the more the system certainty level will be reduced, and the more likely it is that the attack will be blocked when it finally arrives. If the traffic does not appear suspicious, then the system certainty will increase and the system will become more permissive. Accordingly, the present system and method provides a greater likelihood of preventing an attack, while decreasing the probability that legitimate traffic will be blocked. (*Specification*, Page 9, line 15 through Page 10, line 9).

The system certainty level may be adjusted using various formulas. For example, a formula which increases in value as more non-matching data is received, and decreases in value as matching data is received would be suitable. An example of a formula for determining the certainty level is:

bytes_of_non_matching_data_received / bytes_of_matching_data_received (1)

As each packet is found to not match any signature, the number of bytes in the packet is added to bytes_of_non_matching_data_received. For each packet that is found to match a signature, the number of bytes in its packet is added to bytes_of_matching_data_received. Accordingly, as matching data is received, the certainty level goes down, and as nonmatching data is received, the certainty level goes up. Of course, variations of the above noted formula may be used. For example, the maximum and/or minimum certainty levels may be bounded to some value, the bytes_of_non_matching_data_received or byted_of_matching_data_received may be multiplied by some constant, the packet count may be added instead of the byte count, etc. (*Specification*, Page 10, line 10 through Page 11, line 2).

Another embodiment of the present disclosure will be described by reference. to Figure 5, which is a flow chart of a method for maintaining computer security according to another embodiment of the present disclosure. According to this embodiment, instead of increasing the system certainty level each time it is determined that the data does not match a signature in the database, the system certainty level is periodically set to its initial value after a predetermined amount of time has elapsed. For example, the system certainty level may be a fixed value or may be set by presenting a user with a graphic user interface (GUI) prompting the user to set the initial system certainty level. If a user is aware that a particular type of malicious code has been introduced to the internet, the user can set the system certainty level to a low system certainty level, thus making the system less permissive and more likely to catch and prevent an attack. An elapsed time clock is started to keep track of the elapsed time from when the system is started. The incoming data (e.g., data packet) is received and compared with the signatures in database (Step S60). If the data does not match a signature found in the signature database (No, Step S62), the data is allowed to pass. If a match is found in the signature database 402 (Yes, Step S62), then the certainty level of the system 303 is decreased (Step S63). The signature certainty level is then compared to the system certainty level (Step S68). If the signature certainty level is greater than the system certainty level (Yes, Step S60), then the data 401 is discarded (Step S64). For example, the data may be discarded to a bit bucket. If after decreasing the system certainty level, the signature certainty level is not greater than the signature certainty (No, Step S60), then the data 401 is forwarded on (Step S62). After the data is discarded or passed, the system then determines whether a predetermined time has elapsed (Step S66). If the predetermined time has not elapsed (No, Step S66), no action is taken. The system then waits for the next packet of data (Step S68). If a predetermined time has elapsed (Yes, Step S66), the system certainty level is reset to its initial value (Step S70), the elapsed time is restarted and the system waits for the next packet of data (Step S68). (*Specification*, Page 11, line 3 through Page 12, line 5).

Each time the system tests subsequent data, the decreased system certainty level set by the previous data becomes the new system certainty level. The more suspicious activity the system receives, the more the system certainty level will be reduced, and the more likely it is that the attack will be blocked when it finally arrives. If some suspicious traffic has occurred, but not enough has occurred within the predetermined amount of time, it is likely

that an attack will not occur shortly and the system certainty will be reset to its initial value and the system will again become more permissive. Accordingly, the present system and method provides a greater likelihood of preventing an attack, while decreasing the probability that legitimate traffic will be blocked. (*Specification*, Page 12, lines 6-14).

With regard to the independent claims currently under Appeal, Appellant provides the following concise explanation of the subject matter recited in the claim elements. For brevity, Appellant does not necessarily identify every portion of the Specification and drawings relevant to the recited claim elements. Additionally, this explanation should not be used to limit Appellant's claims but is intended to assist the Board in considering the Appeal of this Application.

For example, independent Claim 1, as appealed, recites:

> A computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit (i.e., Figure 1, reference numerals 100, 102, and 104; Figure 3, reference numeral 303; Figure 4, reference numerals S40-S54; Page 7, lines 6-18; Page 9, line 4 through Page 11, line 2), comprises:
>
> determining an initial system certainty value for the computer system (i.e., Figure 3, reference numeral 402-404; Page 9, lines 7-11);
>
> providing access to a database of signatures, each signature including a signature certainty value (i.e., Figure 3, reference numerals 402-404; Figure 4, reference numerals S40; Page 9, lines 7-11);
>
> receiving data (i.e., Figure 3, reference numerals 401; Figure 4, S40; Page 9, lines 7-11);
>
> comparing the received data with the database of signatures (i.e., Figure 3, reference numeral 404; Figure 4, reference numeral S40; Page 9, lines 7-11);
>
> increasing the system certainty value if the received data does not match a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S44; Page 9, lines 11-14);
>
> decreasing the system certainty value if the received data matches a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S46; Page 9, lines 15-16); and
>
> filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data (i.e. Figure 3, reference numeral 406; Figure 4, reference numeral S48; Page 9, lines 16-22).

As another example, independent Claim 7, as appealed, recites:

> A system for maintaining computer security (i.e., Figure 1, reference numerals 100, 102, and 104; Figure 3, reference numeral 303;

Figure 4, reference numerals S40-S54; Page 7, lines 6-18; Page 9, line 4 through Page 11, line 2), comprising:

means for determining an initial system certainty value for the computer system (i.e., Figure 3, reference numeral 402-404; Page 9, lines 7-11);

means for providing access to a database of signatures, each signature including a signature certainty value (i.e., Figure 3, reference numerals 402-404; Figure 4, reference numerals S40; Page 9, lines 7-11);

means for receiving data (i.e., Figure 3, reference numerals 401; Figure 4, S40; Page 9, lines 7-11);

means for comparing the received data with the database of signatures (i.e., Figure 3, reference numeral 404; Figure 4, reference numeral S40; Page 9, lines 7-11);

means for increasing the system certainty value if the received data does not match a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S44; Page 9, lines 11-14);

means for decreasing the system certainty value if the received data matches a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S46; Page 9, lines 15-16); and

means for filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data (i.e. Figure 3, reference numeral 406; Figure 4, reference numeral S48; Page 9, lines 16-22).

As another example, independent Claim 13, as appealed, recites:

A computer recording medium including computer executable code for maintaining security of a computer system (i.e., Figure 1, reference numerals 100, 102, and 104; Figure 3, reference numeral 303; Figure 4, reference numerals S40-S54; Page 7, lines 6-18; Page 9, line 4 through Page 11, line 2), comprising:

code for determining an initial system certainty value for the computer system (i.e., Figure 3, reference numeral 402-404; Page 9, lines 7-11);

code for providing access to a database of signatures, each signature including a signature certainty value (i.e., Figure 3, reference numerals 402-404; Figure 4, reference numerals S40; Page 9, lines 7-11);

code for receiving data (i.e., Figure 3, reference numerals 401; Figure 4, S40; Page 9, lines 7-11);

code for comparing the received data with the database of signatures (i.e., Figure 3, reference numeral 404; Figure 4, reference numeral S40; Page 9, lines 7-11);

code for increasing the system certainty value if the received data does not match a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S44; Page 9, lines 11-14);

code for decreasing the system certainty value if the received data matches a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, S46; Page 9, lines 15-16); and

code for filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data (i.e. Figure 3, reference numeral 406; Figure 4, reference numeral S48; Page 9, lines 16-22).

As still another example, independent Claim 19, as appealed, recites:

A system for maintaining computer security (i.e., Figure 1, reference numerals 100, 102, and 104; Figure 3, reference numeral 303; Figure 4, reference numerals S40-S54; Page 7, lines 6-18; Page 9, line 4 through Page 11, line 2), comprising:

a computer comprising a memory and a central processing unit (i.e. Figure 1, reference numerals 100, 102, and 104; Page 7, lines 6-18), the computer being operable to:

determine an initial system certainty value for the computer system (i.e., Figure 3, reference numeral 402-404; Page 9, lines 7-11);

provide access to a database of signatures, each signature including a signature certainty value (i.e., Figure 3, reference numerals 402-404; Figure 4, reference numerals S40; Page 9, lines 7-11);

receive data (i.e., Figure 3, reference numerals 401; Figure 4, S40; Page 9, lines 7-11);

compare the received data with the database of signatures (i.e., Figure 3, reference numeral 404; Figure 4, reference numeral S40; Page 9, lines 7-11);

increase the system certainty value if the received data does not match a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, reference numeral S44; Page 9, lines 11-14);

decrease the system certainty value if the received data matches a signature in the database (i.e., Figure 3, reference numeral 405; Figure 4, reference numeral S46; Page 9, lines 15-16); and

filter the data based on the system certainty value and the signature certainty value of a signature matching the received data (i.e. Figure 3, reference numeral 406; Figure 4, reference numeral S48; Page 9, lines 16-22).

For example, dependent Claim 3, as appealed, recites:

The method of claim 1, wherein the increased or decreased certainty value becomes the initial system value (i.e., Figure 3, reference numeral 405; Figure 4, reference numerals S44 and S46; Page 9, lines 11-16; Page 10, lines 2-3).

Dependent Claims 9, 15, and 21 recite certain similar claim elements and operations.

For example, dependent Claim 6, as appealed, recites:

The method of claim 5, wherein the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded (i.e. Figure 3, reference numeral 406; Figure 4, reference numeral S48; Page 9, line 22 through Page 10, line 2).

Dependent Claims 12, 18, and 24 recite certain similar claim elements and operations.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Are Claims 1-4, 7-10, 13-16, and 19-22 unpatentable under 35 U.S.C. § 103(a) over *Vaidya* in view of *Coleman?*

Are Claims 5, 11, 17, and 23 unpatentable under 35 U.S.C. § 103(a) over *Vaidya* in view of *Coleman* and further in view of *Nakae*?

Are Claims 6, 12, 18, and 24 unpatentable under 35 U.S.C. § 103(a) over *Vaidya* in view of *Coleman* and *Nakae* and further in view of *Moran*?

ARGUMENTS

The Examiner rejects Examiner rejects Claims 1-4, 7-10, 13-16, and 19-22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,279,113 to Vaidya (*"Vaidya"*) in view of U.S. Patent Publication No. 2005/0037733 to Coleman et al (*"Coleman"*). The Examiner also rejects Claims 5, 11, 17, and 23 under 35 U.S.C. § 103(a) as being unpatentable over *Vaidya* in view of *Coleman*, in view of U.S. Publication No. 20040172557 issued to Nakae et al. ("*Nakae*"); and Claims 6, 12, 18, and 24 under 35 U.S.C. § 103(a) as being unpatentable over *Vaidya* in view of *Coleman*, in view of *Nakae*, and in view of U.S. Patent No. 7,032,114 issued to Moran ("*Moran*").

For at least the following reasons, Appellant respectfully submits that these rejections are improper and should be reversed by the Board.

I. Legal Standard for Obviousness

The question raised under 35 U.S.C. § 103 is whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art at the time of the invention. One of the three basic criteria that must be established by an Examiner to establish a *prima facie* case of obviousness is that "the prior art reference (or references when combined) must teach or suggest ***all the claim limitations***." *See* M.P.E.P. § 706.02(j) citing *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991) (emphasis added). "***All words*** in a claim must be considered in judging the patentability of that claim against the prior art." *See* M.P.E.P. § 2143.03 citing *In re Wilson*, 424 F.2d 1382, 1385 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970) (emphasis added).

In addition, even if all elements of a claim are disclosed in various prior art references, which is certainly not the case here as discussed below, the claimed invention taken as a whole still cannot be said to be obvious without some reason why one of ordinary skill at the time of the invention would have been prompted to modify the teachings of a reference or combine the teachings of multiple references to arrive at the claimed invention.

The controlling case law, rules, and guidelines repeatedly warn against using an Appellant's disclosure as a blueprint to reconstruct the claimed invention. For example, the M.P.E.P. states, "The tendency to resort to 'hindsight' based upon Appellant's disclosure is

often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art." M.P.E.P. § 2142.

The U.S. Supreme Court's decision in *KSR Int'l Co. v. Teleflex, Inc.* reiterated the requirement that Examiners provide an explanation as to why the claimed invention would have been obvious. *KSR Int'l Co. v. Teleflex, Inc.*, 127 S.Ct. 1727 (2007). The analysis regarding an apparent reason to combine the known elements in the fashion claimed in the patent at issue "should be made explicit." *KSR*, 127 S.Ct. at 1740-41. "Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.* at 1741 (internal quotations omitted).

The new examination guidelines issued by the PTO in response to the *KSR* decision further emphasize the importance of an explicit, articulated reason why the claimed invention is obvious. Those guidelines state, in part, that "[t]he key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit." *Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57526, 57528-29 (Oct. 10, 2007) (internal citations omitted). The guidelines further describe a number of rationales that, in the PTO's view, can support a finding of obviousness. *Id.* at 57529-34. The guidelines set forth a number of particular findings of fact that must be made and explained by the Examiner to support a finding of obviousness based on one of those rationales. *See id.*

II. Claims 1-4, 7-10, 13-16, and 19-22 are Allowable over *Vaidya* in view of *Coleman*

The *Final Office Action* rejects Claims 1-4, 7-10, 13-16, and 19-22 under 35 U.S.C. § 103(a) as being unpatentable over *Vaidya* in view of *Coleman*. Appellant respectfully submits that these rejections are improper and should be reversed.

A. Claims 1-2, 4, 7-8, 10, 13-14, 16, 19-20, and 22

Claim 1 of the present Application, as presented on Appeal, recites:

> A computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, comprising:
>
> *determining an initial system certainty value for the computer system*;
>
> providing access to a database of signatures, each signature including a signature certainty value;
>
> receiving data;
>
> comparing the received data with the database of signatures;
>
> *increasing the system certainty value if the received data does not match a signature in the database;*
>
> *decreasing the system certainty value if the received data matches a signature in the database; and*
>
> filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data.

Thus, Appellant's claim recites determining an initial system certainty value for a computer system. Received data is compared with the database of signatures. The system certainty value is increased if the received data does not match a signature in the database. Alternatively, the system certainty value is decreased if the received data matches a signature in the database. It continues to be Appellant's position that the proposed *Vaidya-Coleman* combination does not render obvious at least the above-emphasized steps.

The *Final Office Action* acknowledges that *Vaidya* does not disclose the recited claim elements and instead relies on *Coleman* to disclose the limitations "determining an initial system certainty value for the computer system," "increasing the system certainty value if the received data does not match a signature in the database," and "decreasing the system certainty value if the received data matches a signature in the database." (*Final Office Action*, pages 5-8). Specifically, the *Final Office Action* relies on the "mistrust level for each wireless network device", as discussed in *Coleman*, as disclosing "an initial system certainty value for the computer system" that is recited in Appellant's claim. (*Final Office Action*, pg. 5). Appellant respectfully disagrees.

Coleman relates to a method and system that "provides autonomous wireless intrusion detection and prevention, with minimal or no operator intervention." (*Coleman*, Abstract). Specifically, *Coleman* discloses that a response initiator/adaptive feedback engine (RIAFE) 86 "maintains a running mistrust level for each wireless network device 36, 38 and [wireless access point (WiAP)] 16, 16' in the [Wireless Network (WiNet)] 18 base don WiNet 18 traffic/event data 100 received at [Cooperative Decision Engine (CDE)] 76." (*Coleman*, paragraph 102). Thus, the mistrust levels disclosed in *Coleman* correspond to individual levels associated with each wireless network device located within a computer system. There is no disclosure, teaching, or suggestion of a single initial system certainty value for the computer system. Accordingly, *Coleman* and the proposed *Vaidya-Coleman* combination, as relied upon by the *Final Office Action*, does not disclose, teach, or suggest "determining an initial **system** certainty value for the computer **system**," as recited in Claim 1.

Furthermore, even if one considers the mistrust levels disclosed in *Coleman* to correspond to Appellant's "single initial system certainty value" (a point Appellant does not concede and disputes above), *Coleman* fails to disclose, teach, or suggest the "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database," as recited in Appellant's Claim 1.

While *Coleman* does disclose incrementing and decrementing the mistrust levels assigned to the devices, Appellant respectfully contends that these changes are not based on either matching or not matching signatures. For instance, *Coleman* clearly states throughout that "mistrust level decrementing is accomplished based on three parameters, described as follows: (1) a decrement timer D1 exceeds a mistrust level decrement interval from the operational protection suite; (2) mistrust level four has been reached, the wireless network device 36, 38 successfully re-authenticates, and re-login is also successful; (3) manual intervention 90 from the network administrator 92." (*Coleman*, paragraph 0121). Therefore, *Coleman* discloses a decrementing step based only on timing, manual intervention, or re-authentication. With regard to the decrementing of a mistrust level, *Coleman* discloses:

> A decrement timer D1 is maintained on the RIAFE 86 for each WiAP 16 or wireless network device 36,38 . . . whose mistrust level exceeds zero. The decrement timer is reset whenever an anomalous event occurs at the given wireless network device, or when the operational protection suite is cycled. The mistrust level is decremented in the following way: if the decrement timer exceeds the mistrust level decrement interval from the

> operational protection suite, or if mistrust level four has been reached and the wireless network device 36, 38 successfully re-authenticates and there is successful login on the wireless device, then the mistrust level for that device is decremented by one.
>
> At any time, the network administrator 92 may manually reset the mistrust level for a given wireless network device 36, 38 or WiAP 16 to any value. Through these specific mechanisms, the mistrust levels are selectively decremented by the RIAFE 86 and wireless network devices 34, 36 or WiAP 16 can return to a stable, innocuous condition if anomalous events cease to occur.

(*Coleman*, paragraphs 123-124). Thus, *Coleman* merely discloses decrementing the mistrust level if a predetermined amount of time passes and no anomalous event is detected, if the device is reauthenticated, or if the network administrator intervenes. There is no disclosure, teaching, or suggestion that matching or not matching a signature plays any role in this step.

In response to these arguments, the *Final Office Action* states "'matching signatures' specifically the 'signatures' can be any criteria that are deemed as an intrusion that is then matched or determined to be a known intrusion." (*Final Office Action*, page 13). The *Advisory Action* further states that decrementing could be based on "any event that would trigger a responsive action." (*Advisory Action*, page 2). Despite these unsupported assertions, Appellant respectfully maintains that *Coleman* discloses "decrementing" based only on the three criteria listed above. This fails to disclose a decrementing step based on "any criteria that are deemed as an intrusion that is then matched." Therefore, even under the Office Action's proposed "broadest" interpretation, this cited portion fails to disclose, teach, or suggest "decreasing the system certainty value if the received data matches a signature in the database," as recited in Claim 1.

For at least these reasons, Appellant respectfully submits that the rejection of Claim 1 is improper and request that the rejection be withdrawn. For analogous reasons, Appellant also submits that the rejections of independent Claims 7, 13, and 19 are improper and request that these rejections also be withdrawn. Accordingly, Appellants respectfully request favorable action with regard to independent Claims 1, 7, 13, and 19, together with the claims depending on these claims (including at least Claims 2, 4, 8, 10, 14, 16, 20, and 22).

B. Claims 3, 9, 15, and 21

Claims 3, 9, 15, and 21 depend from Claims 1, 7, 13, and 19, respectively. As shown above, Appellant respectfully contends that the proposed *Vaidya-Coleman* combination fails to disclose, teach, or suggest every limitation of these independent base claims. As such, Appellant respectfully contends that Claims 3, 9, 15, and 21 are allowable over the cited references at least as a result of their respective dependencies upon allowable independent Claims 1, 7, 13, and 19.

Additionally, Claims 3, 9, 15, and 21 recite claim elements that further distinguish over the art. For example, Claim 3 recites that "the increased or decreased certainty value becomes the initial system value." Again, the *Final Office Action* relies on *Coleman* to disclose the recited claim elements. (*Final Office Action*, page 8). Appellant respectfully disagrees.

First of all, as discussed above with regard to Claim 1, *Coleman* fails to disclose, teach, or suggest a "**system** certainty value." Rather, the mistrust levels disclosed in *Coleman* correspond to individual levels associated with each wireless network device located within a computer system. (*Coleman*, paragraph 102). Furthermore, the cited portion of *Coleman* merely discloses that the mistrust level for individual network devices is "initialized to zero, then incremented and/or decremented." (*Coleman*, paragraph 0102). Specifically, *Coleman* discloses that "mistrust level decrementing is accomplished based on three parameters, described as follows: (1) a decrement timer D1 exceeds a mistrust level decrement interval from the operational protection suite; (2) mistrust level four has been reached, the wireless network device 36, 38 successfully re-authenticates, and re-login is also successful; (3) manual intervention 90 from the network administrator 92." (*Coleman*, paragraph 0121). Thus, *Coleman* merely discloses decrementing the mistrust level if a predetermined amount of time passes and no anomalous event is detected, if the device is reauthenticated, or if the network administrator intervenes. With regard to the actual decrementing of the mistrust level, *Coleman* provides an Equation 9 for calculating the new mistrust level. (*Coleman*, paragraph 118). The equation takes into account the old mistrust level, a weighted anomaly, and a mistrust level decrement value. Thus, the new mistrust level is calculated using a predetermined calculation having multiple variables. There is no disclosure that "the increased or decreased certainty value becomes the initial system value," as recited in Claim 3.

For at least these reasons, Appellant respectfully submits that the rejection of dependent Claim 3 is improper and request that the rejection be withdrawn. For analogous reasons, Appellant also submits that the rejections of dependent Claims 9, 15, and 21 are improper and should also be withdrawn.

III. Claims 5, 11, 17, and 23 are Allowable over the Proposed *Vaidya- Coleman-Nakae* Combination

Claims 5, 11, 17, and 23 depend from Claims 1, 7, 13, and 19, respectively. As shown above, Appellant respectfully contends that the proposed *Vaidya-Coleman* combination fails to disclose, teach, or suggest every limitation of these independent base claims. As such, Appellant respectfully contends that Claims 5, 11, 17, and 23 are allowable over the cited references at least as a result of their respective dependencies upon allowable independent Claims 1, 7, 13, and 19. Accordingly, Appellant requests reconsideration and allowance of Claims 5, 11, 17, and 23.

IV. Claims 6, 12, 18, and 24 are Allowable over the Proposed *Vaidya-Coleman-Nakae-Moran* Combination

Claims 6, 12, 18, and 24 depend from Claims 1, 7, 13, and 19, respectively. As shown above, Appellant respectfully contends that the proposed *Vaidya-Coleman* combination fails to disclose, teach, or suggest every limitation of these independent base claims. As such, Appellant respectfully contends that Claims 6, 12, 18, and 24 are allowable over the cited references at least as a result of their respective dependencies upon allowable independent Claims 1, 7, 13, and 19.

Additionally, Claims 6, 12, 18, and 24 recite claim elements that further distinguish over the art. For example, Claim 6 recites that the step of forwarding further comprises "generating a message log to indicate that data matching a signature was forwarded." In the *Final Office Action*, the Examiner admits that *Vaidya*, *Coleman*, and *Nakae* fail to disclose this limitation and relies instead on *Moran*. Appellant respectfully disagrees.

The cited portion discloses "a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file." (*Moran*, Column 4, lines 28-31). While this discloses identifying time steps in a log file, *Moran* fails to disclose, teach, or suggest actually generating a log file, much less a log file that indicates that data matching a signature was forwarded. Accordingly, *Moran* and the proposed *Vaidya-Coleman-Nakae-Moran* combination fails to disclose, teach, or suggest "wherein the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," as recited in Claim 6.

For at least these reasons, Appellant respectfully submits that the rejection of dependent Claim 6 is improper and request that the rejection be withdrawn. For analogous reasons, Appellant also submits that the rejections of dependent Claims 12, 18, and 24 are improper and should also be withdrawn.

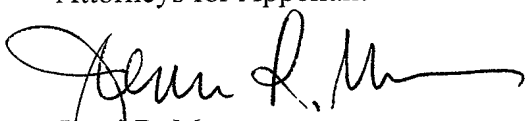
CONCLUSION

Appellant has demonstrated that the present invention, as claimed, is clearly distinguishable over the prior art cited by the Examiner. Therefore, Appellant respectfully requests the Board to reverse the final rejections and instruct the Examiner to issue a Notice of Allowance with respect to all pending claims.

The Commissioner is hereby authorized to charge $540.00 for filing this Brief in support of an Appeal to Deposit Account No. 02-0384 of Baker Botts, L.L.P. No other fees are believed due; however, the Commissioner is authorized to charge any additional fees or credits to Deposit Account No. 02-0384 of Baker Botts, L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Appellant



Jenni R. Moen
Reg. No. 52,038
(214) 415-4820

Dated: November 15, 2010

Correspondence Address:

at Customer No. **05073**

APPENDIX A:

1. A computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, comprising:

determining an initial system certainty value for the computer system;

providing access to a database of signatures, each signature including a signature certainty value;

receiving data;

comparing the received data with the database of signatures;

increasing the system certainty value if the received data does not match a signature in the database;

decreasing the system certainty value if the received data matches a signature in the database; and

filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data.

2. The method of claim 1, wherein the data that does not match a signature in the database is forwarded to its destination.

3. The method of claim 1, wherein the increased or decreased certainty value becomes the initial system value.

4. The method of claim 1, wherein the data comprises a packet of data.

5. The method of claim 1, wherein the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value; and discarding the data if the signature certainty value is greater than the system certainty value.

6. The method of claim 5, wherein the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded.

7. A system for maintaining computer security, comprising:

means for determining an initial system certainty value for the computer system;

means for providing access to a database of signatures, each signature including a signature certainty value;

means for receiving data;

means for comparing the received data with the database of signatures;

means for increasing the system certainty value if the received data does not match a signature in the database;

means for decreasing the system certainty value if the received data matches a signature in the database; and

means for filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data.

8. The system of claim 7, wherein the data that does not match a signature in the database is forwarded to its destination.

9. The system of claim 7, wherein the increased or decreased certainty value becomes the initial system value.

10. The system of claim 7, wherein the data comprises a packet of data.

11. The system of claim 7, wherein the means for filtering further comprises means for forwarding the data if the signature certainty value is less than the system certainty value; and discarding the data if the signature certainty value is greater than the system certainty value.

12. The system of claim 11, wherein the means for forwarding further comprises means for generating a message log to indicate that data matching a signature was forwarded.

13. A computer recording medium including computer executable code for maintaining security of a computer system, comprising:

code for determining an initial system certainty value for the computer system;

code for providing access to a database of signatures, each signature including a signature certainty value;

code for receiving data;

code for comparing the received data with the database of signatures;

code for increasing the system certainty value if the received data does not match a signature in the database;

code for decreasing the system certainty value if the received data matches a signature in the database; and

code for filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data.

14. The computer recording medium of claim 13, wherein the data that does not match a signature in the database is forwarded to its destination.

15. The computer recording medium of claim 13, wherein the increased or decreased certainty value becomes the initial system value.

16. The computer recording medium of claim 13, wherein the data comprises a packet of data.

17. The computer recording medium of claim 13, wherein the code for filtering further comprises code for forwarding the data if the signature certainty value is less than the system certainty value; and discarding the data if the signature certainty value is greater than the system certainty value.

18. The computer recording medium of claim 17, wherein the code for forwarding further comprises code for generating a message log to indicate that data matching a signature was forwarded.

19. A system for maintaining computer security, comprising:

a computer comprising a memory and a central processing unit, the computer being operable to:

determine an initial system certainty value for the computer system;

provide access to a database of signatures, each signature including a signature certainty value;

receive data;

compare the received data with the database of signatures;

increase the system certainty value if the received data does not match a signature in the database;

decrease the system certainty value if the received data matches a signature in the database; and

filter the received data based on the system certainty value and the signature certainty value of a signature matching the received data.

20. The system of claim 19, wherein if the received data does not match a signature in the database, the received data is forwarded to an intended destination.

21. The system of claim 19, wherein the increased or decreased system certainty value becomes the initial system certainty value.

22. The system of claim 19, wherein the data comprises a packet of data.

23. The system of claim 19, wherein the computer is further operable to:

forward the received data if the signature certainty value is less than the system certainty value; and

discard the received data if the signature certainty value is greater than the system certainty value.

24. The system of claim 23, wherein the computer is further operable to generate a message log to indicate that received data matching a signature was forwarded.

APPENDIX B

Evidence Appendix

No other evidence was submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 entered by the Examiner and relied upon by Appellant in the Appeal.

APPENDIX C

Related Proceedings Appendix

As stated on Page 3 of this Appeal Brief, there are no known interferences or judicial proceedings that will directly affect or be directly affected by or have a bearing on the Board's decision regarding this Appeal.